ABSTRACT OF THE DISCLOSURE

Expanded key schedule circuit for common key encryption system in which expanded keys are used in a predetermined order in data randomizing process for encryption and in a reversed order in data randomizing process for decryption, comprises round processing circuits connected in series. The round processing circuits subject the common key or sub key of a previous stage to a round function to output a sub key. The sub key of the last stage is equal to the common key. The expanded keys are generated from the sub keys.